R 172310Z JUN 09
FM AMEMBASSY CANBERRA
TO SECSTATE WASHDC 1641
INFO AMCONSUL MELBOURNE
AMCONSUL PERTH
AMCONSUL SYDNEY
DEPT OF HOMELAND SECURITY CENTER WASHINGTON DC

C O N F I D E N T I A L CANBERRA 000568

DEPARTMENT FOR S/CT FOR HILLARY BATJER JOHNSON AND PAUL SCHULTZ, AND DS/IP/EAP FOR GEORGE LAMBERT, NCTC

E.O. 12958: DECL: 06/18/2034
TAGS: ASEC CVIS KVPR PGOV PREL PTER
SUBJECT: GOVERNMENT OF AUSTRALIA-INFORMATION COLLECTION, SCREENING AND SHARING

REF: A. 06 STATE 190832
¶B. 07 STATE 133921
¶C. 08 STATE 048120
¶D. 09 STATE 32287

Classified By: Charge d'Affaires a.i. Daniel Clune for reason 1.4(b) and (c)

¶1. (U) The Australian government is forward leaning in both maintaining border security and providing assistance to partners in the fight against terrorism. To that end, robust and dynamic protocols are in place to ensure that the movement of suspected and known terrorists are monitored and thwarted. This has been and continues to be a whole-of-government effort. In response to State 133921, post submits the following information on GOA practices with regard to information collection, screening and sharing.

BEGIN EXTRACT

¶2. (C)A. Watch listing:

The Australian Customs and Border Protection Service (Customs and Border Protection) maintains a watch list and works closely with intelligence and law enforcement parQrs to ensure that border security is maintained through the sharing of intelligence and other available information. Information is shared within the parameters of Australia's privacy legislation.

Immigration maintains the Central Movement Alert List. This list hosts identities of concern ranging from immigration malpractice, criminals, war crimes and national security concerns. The Document Alert List component of CMAL contains details of travel documents of concern. CMAL operates against all visa issuing processes, during check-in using Australia's Advance Passenger Processing (APP) system and is able to prevent travel by refusing boarding permission.

Immigration also coordinates the Regional Movement Alert System (RMAS) - a joint system shared between Australia, the US and New Zealand and focused on lost and stolen travel documents.

¶B. Traveler Information Collection:

Customs and Border Protection uses Passenger Name Record (PNR) information from airlines' reservation and departure control systems to risk assess passengers before arrival. Analysis of PNR and other relevant data plays a critical role in the identification of possible persons of interest in the context of counter-terrorism, drug trafficking, identity fraud, people smuggling and other serious transnational crimes. PNR data provided by airlines includes name and address details, ticketing, check in, seating, form of payment, travel itinerary and baggage information. PNR information is shared with other Australian government agencies within the confines of Australia's privacy

legislation and obligations under international treaties.

In addition to PNR data, Customs and Border Protection receives advance passenger information (API) data from the Department of Immigration and Citizenship (DIAC) for most passengers and crew. This data includes information on identity, passports, other travel documents and flight details. For military and charter flight operators that are not subscribers to the DIAC system, this information is provided directly to Customs and Border Protection. Australia implemented mandatory API reporting in January 2003 for operators of international passenger aircraft and cruise ships traveling to or transiting Australia. In March 2009, legislative amendments introduced provisions that enable infringement notices to be issued, in lieu of prosecution, to air and sea carriers that breach mandatory API reporting requirements. This measure seeks to strengthen the integrity of Australia's borders and to provide carriers an option to improve compliance without resorting to court action. This infringement regime will be implemented during 2009-10.

¶C. Border Control and Screening:

Customs and Border Protection officers exercise a diverse range of powers, the authority for which is legislatively based. TQe powers are directed to the agency's border control and aviation security responsibilities. Customs and Border Protection officers' powers include powers to question, search, examine, detain, board and arrest. Customs and Border Protection is also a clearance authority under Australia's Migration Act 1958 and performs the clearance function at airports and ports on behalf of DIAC. Cases of concern are referred for processing to DIAC specialist staff who are able to refuse entry clearance to persons of concern and also initiate more complex responses (for example protection claims by asylum seekers).

Customs and Border Protection works closely with other border management agencies including DIAC, Australian Quarantine and Inspection Service (AQIS), Australian Federal Police (AFP), the Department of Infrastructure, Transport, Regional Development and Local Government (Infrastructure) and intelligence agencies in relation to border control and screening.

As part of Australia's border security management process, all applicants who apply for an Australian visa are required to meet relevant health character and security requirements.

In order to facilitate security requirements, DIAC manages the Security Referral Service (SRS) which provides a systems connectivity between DIAC and the competent Australian intelligence authorities.

Some visa applicants undertake in depth security assessments prior to visa issue.

The SRS has been directly attributed to significant reduction in average security referral processing times. The SRS also has well developed reporting mechanisms which allow for transparent reporting

¶D. Biometric Collection

Through the Australian Passport Office, the Department of Foreign Affairs and Trade (DFAT) provides passport services to Australians. In 2005, Australia committed 67.5 million dollars to the development of Biometric technology in the Australian Passport, including a Facial Recognition system to support biometric matching. Since October 2005, all Australian ePassports contain a chip which stores the applicant's personal data (i.e. name, date of birth, nationality and passport number). It also holds a photo of the applicant that can be used for facial recognition, which is the primary biometric identifier used in Australian border management processes. As at May 2009, over 11 million biometric images are stored within the DFAT Facial Recognition system and 4.9 million ePassports are in

circulation (approx 49 percent of total passports in circulation).

Australia's automated border control system, SmartGate, is a program that allows ePassports to be read at kiosks which utilize facial recognition to process travelers. Smartgate has now been deployed for arriving Australian and New Zealand ePassport holders, over 18 years of age, at five of Australia's international airports. SmartGate kiosks have also been installed at Auckland International Airport in New Zealand to allow eligible travelers to complete the first step in border processing prior to departing for Australia.

DIAC currently collects fingerprints from persons in immigration detention, including illegal foreign fishers.

¶E. Passports

All Australian Passports have chips that comply with standards sets by the International Civil Aviation Organization (ICAO). In addition to basic access control, the N Series Passport (released in May 2009) incorporates Active Authentication technology to detect attempts to fraudulently clone or copy the chip. The data contained on the chip can be accessed only after the Machine Readable Zone at the base of the document has been successfully read.

As part of the chip writing process, the information on the chip is "signed" using a Public Key Infrastructure (PKI) certificate and a copy of the public certificate is then written to the chip. The chip is then locked to prevent tampering. Any tampering with the chip would be detected through the certificate validation process. The Customs SmartGate border system also uses this technology to validate Australian ePassports at the border.

Replacement passports are issued for full validity. According to DFAT, if an Australian citizen qualifies for a passport he rightly qualifies for full validity. In cases where an applicant's citizenship is not in question but they fail to meet the requirements for full validity, a limited validly emergency passport can be issued. These passports contain only a few visa pages, are normally valid for seven months and contain no chip.

- Repeat passport losers pay a fee for each lost passport in a 5 year period. The fee for the first lost passport is 69 dollars, the second is 208 dollars, the third 416 dollars and the fourth 416 plus a replacement valid for only five years. This is in addition to normal processing fees.

- There is no difference in appearance or size of replacement passports.

- GOA has not/not noticed a trend towards "clean" passports.

¶F. Fraud Detection

The Passport Fraud Section (PFS) of the Australian Passport Office retains fraudulent and damaged documents for examination and analysis of trends. PFS has established an electronic register to assist this analysis. Some fraudulent documents are retained for training and exhibit purposes. Others deemed to have no future value are destroyed.

DIAC maintains forensic document examiners at all major ports of entry and also trains its Airline Liaison Officers (stationed at major hubs off-shore), overseas compliance officers (stationed at diplomatic posts) and border personnel from regional countries to facilitate more effective detection of fraudulent travel documents.

DIAC also maintains a global intelligence database (IMtel). This provides access to all DIAC staff (including off-shore) to document alerts, fraud reporting, general immigration intelligence and analytical reports generated by DIAC staff or received from allied countries. IMtel also provides real-time analytical tools and supports global working on

cases of concern.

¶G. Freedom of Information

Intelligence and security agencies are exempt from Australia's Freedom of Information Act 1982 (FOI Act). Documents that have originated with, or been received from, certain agencies, such as the Australian Security Intelligence Organization (ASIO), are exempt from this legislation. (Such documents, however, fall within the public access regime of the Archives Act 1983 once they reach 30 years old; and while exemptions may be sought, they are subject to a statutory appeal process.) Agencies that are subject to the FOI Act must respond to FOI requests, in accordance with the provisions of that legislation.

Decisions to refuse access to documents can be subject to internal review by the agency and then external review.

Non-citizens can make requests under the FOI Act. However, one of the requirements for a valid FOI request is an address in Australia for the service of documents.

Further information on the FOI Act, including proposed reforms, is available from the Australian Government Department of the Prime Minister and Cabinet's website www.pmc.gov.au/foi

¶H. Privacy

The Privacy Act 1988 (Privacy Act) gives effect to Australia's obligations under Article 17 of the International Covenant on Civil and Political Rights as well as its agreement to implement Guidelines adopted in 1980 by the Organization for Economic Cooperation and Development (OECD) for the Protection of Privacy and Trans-border Flows of Personal Data. It applies to residents, both citizens and non-citizens alike and to both the public and private sectors. Most State and both Territory Governments have their Qsectors. Most State and both Territory Governments have their own privacy laws.

The Act provides for the protection of personal information in the possession of federal government departments and agencies and private sector organizations with an annual turnover of $3m . It gives individuals a right to know what information an agency or organization holds about them and a right to correct that information if it is wrong; and it provides for complaints handling and allows for the Privacy Commissioner to make determinations, including for compensation, where breaches of privacy are found.

The Privacy Commissioner also has functions in the areas of credit reporting, data matching, and spent convictions.

The Australian Government is currently considering recommendations to reform the Privacy Act and will respond in two stages over the next two years (2010-11).

END EXTRACT

¶3. (SBU) FURTHER INFORMATION ON IMMIGRATION PROCESSES

Australia has a non-discriminatory immigration program and a universal visa system that requires all non-citizens to obtain a visa before entering Australia. Visitors to Australia from the United States and some thirty other countries are eligible to apply for an Electronic Travel Authorization (ETA) through a travel agent, airline, Australian visa office, or other approved service provider. In certain cases, the application may be completed online. The Australian Department of Immigration and Citizenship (DIAC) is the competent authority for issuing visas.

When entering Australia, the Australian Migration Act 1958 requires citizens and non-citizens to identify themselves to a clearance authority and to provide certain information in

order to enter Australia. This process is designed to regulate the entry of people to Australia and to ensure that those who enter have the authority to do so, that they are who they claim to be, and that they provide other information if required.

Under this process, the clearance authority examines a person's authority to enter Australia and checks that the person is an Australian citizen, a visa holder or a person eligible for a visa in immigration as well as the person's travel document.

The Australian Migration Act 1958 allows for fines of up to AUD $10,000 for the master, owner, agent, charter and operator or agent of a vessel that carries any non-visaed person to Australia. As a matter of policy, DIAC may issue infringement notices for up to AUD $5000 for the same offense, where organized malpractice is not an issue.

In March 2009, legislative amendments introduced provisions that enable infringement notices to be issued, in lieu of prosecution, to air and sea carriers that breach mandatory API reporting requirements. This measure seeks to strengthen the integrity of Australia's borders and to provide carriers an option to improve compliance without resorting to court action. From l July 2009, this infringement regime will be implemented in respect of airlines that fail to provide advance reports on airline passengers and crew. The implementation date for cruise ships is to be confirmed.

Australia's border management system is based on a number of 'layers', as follows:

1) Australia's Universal Visa System

Australia's universal visa system is the first line of defense against the entry of people who pose a security, criminal or health risk. All non-citizens are required to hold a current visa to enter and stay in Australia.

2) Overseas Compliance Officers (OSCOs)

OSCOs are specialist immigration compliance officers located in high immigration risk regions overseas whose job is to identify and respond to immigration malpractice. They work closely with visa officers to detect and combat fraud in visa caseloads. As at 1 June 2009, there are 28 OSCOs at 21 posts in 18 countries.

3) Immigration Alert Checking

The Movement Alert List (MAL) is DIAC's principal electronic alert system and forms an integral part of Australia's national security and border control strategy. MAL consists of a Person Alert List (PAL) and a Document Alert List (DAL).

The purpose of MAL is to alert DIAC's decision makers to information the Department holds about an individual during the processing of visa and citizenship applications, passenger processing at overseas check-in points (eg. airports) and immigration clearance at the Australian border.

As at the end of May 2009, there were approximately 700,000 identities listed on the PAL. People may be listed on MAL when they have serious criminal records. Other people listed include those whose presence in Australia may constitute a risk to the Australian community and people who may not enter Australia as they are subject to exclusion periods prescribed by migration legislation. This can occur for a number of reasons, including health concerns, debts owed to the Commonwealth or other adverse immigration records.

As at the end of May 2009, there were about 1.85 million documents (i.e. lost, stolen or fraudulently altered are also recorded on the DAL.

Details identifying people of concern are recorded on MAL as a result of the Department's liaison with law enforcement agencies and departmental offices in Australia

and overseas.

Central MAL (CMAL) ensures that the management of the MAL, and the matching of potential visa and citizenship applicants against individuals and/or documents of concern on the PAL or DAL, is undertaken in a purpose designed center of excellence using specialized analysts, state of the art technology and the most sophisticated name search software, operating 24/7. CMAL ensures:

- All clients are checked against the most up to date version of the movement alert list, at the time of application instead of after a visa has been granted.

- That there is a once-only need for human assessment of possible MAL matches for each client unless new information is received.

- That DIAC decision makers now receive a visible, up to date MAL Status for each client in the Department's visa/citizenship processing systems in real time. If there is a MAL true match a decision on entry is taken by the Department in consultation with any other relevant agency.

The Regional Movement Alert System (RMAS) enables participating APEC economies to verify the status of passports in real-time at the source, alerting the relevant agencies if action is required. These checks are conducted in real-time against passport databases owned and managed by the respective document issuing authorities of the participating APEC economies. RMAS is an initiative of the APEC Business Mobility Group. It currently involves Australia, the United States of America and New Zealand.

4) Advance Passenger Processing (APP)

Australia's Advance Passenger Processing (APP) system is the next layer in Australia's approach to border management. Under this system, all airlines and cruise ships must provide DIAC with information on all passengers and crew, including transit passengers, traveling to or via Australia, as required under the Migration Act. This information is collected at check-in through the APP system and is transmitted to Australia for use by border agencies prior to the arrival of the vessel. The data transmitted to Australia is cross-checked against Australia's immigration databases, as well as alert systems such as DAL and RMAS.

The APP system also assists airlines by enabling them to check if a passenger has authority to travel to Australia, such as a valid visa or Australian passport. This helps to reduce the incidence of airlines carrying inadmissible or inadequately documented passengers to Australia.

APP checking occurred in about 99.8 per cent of all passenger and crew air arrivals during 2007-08. Since 2004, international cruise ships have used the APP system to check more than 174,000 passengers and 98,000 crew. This represents over 99 per cent of cruise ship arrivals with only minor administrative errors affecting 100 per cent compliance. During 2007-08, more than 55,900 passengers and 31,000 crew were APP reported by cruise ships.

5) Airline Liaison Officers (ALOs)

ALOs play a key role in protecting Australia's borders by preventing and deterring irregular movement of people in the region. ALOs conduct document screening of many Australia-bound passengers at key international gateways. They also provide advice to airlines and host governments on passenger documentation issues, and by their visible presence, deter the activities of those involved in people smuggling. ALOs assist airline check-in staff with training and advice about Australia's entry requirements.

There are currently (as at October 2008) 18 ALOs at 11 overseas locations, although this number remains flexible to enable response to changing situations. In 2007-08,

Australian ALOs interdicted 143 irregularly documented Australia-bound travelers.

6) Immigration Inspectors at Australia's Border

In Australia's layered approach to border processing, the border is the final point at which a person's identity and authority to remain in Australia can be confirmed prior to their entry into the community.

Upon arrival at Australia's border, the Migration Act 1958 requires citizens and non-citizens to identify themselves to a clearance authority and provide certain information to enter Australia. This process is designed to regulate the entry of people to Australia and to ensure that those who enter have the authority to do so, that they are who they claim to be and that they provide other information if required.

In 2007-08, there were a total of 25.7 million passenger and crew arrivals and departures. This figure comprises 23.6 million air passengers, 1.3 million air crew, 90,000 sea passengers and 700,000 sea crew. 1,612 people were refused entry at Australia's air and seaports during 2007-08.

¶4. (C) There are no political barriers to further cooperation with the U.S. with regard to data sharing between GOA and the U.S.; the program is in place and active. GOA legal system offers sufficient safeguards for the protection and non-disclosure of information. Information sharing between GOA agencies is consistent with information sharing between government agencies in the U.S.

¶5. (C) GOA defines terrorism under section 100.1 of the criminal code as an act done or a threat made with the intention of advancing a political, religious or ideological cause; and the act is done or the threat is made with the intention of coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or intimidating the public or a section of the public.